Engineering Management
Field Project

Integrated Compliance Framework for Data Processing Applications

By

Jéan Vil

Fall Semester, 2009

An EMGT Field Project report submitted to the Engineering Management Program
and the Faculty of the Graduate School of The University of Kansas
in partial fulfillment of the requirements for the degree of
Master's of Science

_____
Tom Bowlin
Committee Chairperson

_____
John Bricklemyer
Committee Member

_____
Ray Dick
Committee Member

Date accepted: _____

Acknowledgments

The regulatory tornado and industry mandates that have thumped the data processing environment for years have caused companies and information security professionals alike endless angst. As a compliance analyst, I have experienced first hand the challenges with maintaining compliance throughout an organization. Harmonizing the controls that support a company's core businesses has always been an area of interest. The concept of assembling an integrated compliance framework for data processing applications was birthed out of my own challenge to keep up with the number of regulations and industry mandates that are released year after year.

I would like to sincerely acknowledge the University of Kansas and the Engineering Management staff who have instituted this infrastructure allowing graduate students like myself to embark on such research. In particular, a big THANK YOU! to those instructors who have offered plentiful feedback on this work.

I am also truly appreciative of the support that I have received from my employer and my family in completing this program.

Last but not the least; I would like to express my gratitude to the many students at the University that have given un-selfishly of their resources (time and knowledge) to assist me throughout this journey.

Executive Summary

The consumerization and decentralization of information in the last fifteen to twenty years have introduced new challenges that data processing companies must cope with in an effort to survive. To remain compliant in this ever changing business environment, companies' internal information technology controls around policies, processes, and systems must be mapped across regulations, standards, industry mandates, and best practices. Publicly traded businesses have struggled for years to keep-up with the virtual alphabet soup of compliance requirements resulting from new regulations and/or industry mandates. They have, in many cases, built costly and ineffective models to remain in compliance each time a new regulation, a new industry mandate, or a new vulnerability surfaces.

The "Integrated Compliance Framework for Data Processing Applications" makes this whole complex compliance process much easier by focusing on the commonalities in the regulations, standards, and guidelines. It harmonizes controls across the information technology industry to significantly reduce the cost associated with meeting compliance and security requirements effectively and efficiently. It aligns key technical controls with specific requirements that most companies must comply with. Companies facing multiple regulations such as the Sarbanes Oxley Act of 2002, privacy requirements based on the Health Insurance Portability and Accountability Act, Payment Card Industry Data Security Standards mandates, Customer Proprietary Network Information regulation, Personal Identifiable Information regulation, etc. can immediately streamline their compliance measurement processes on a single platform.

This framework facilitates the institutionalization of compliance in the core components of the business model. It allows organizations to focus on a strategic plan to comply with multiple regulatory bodies using the same team, tools, and funding. To this end, the framework assists with: mapping the overlap between multiple regulations and mandates, creating a critical control list for each impact zone, and clarifying any conflicts created by overlapping regulation and mandates.

A robust, systemic, integrated, and well architected compliance framework can help companies comply with complex regulation, as well as spur productivity, enhance customer service, and boost return on technology investment.

Table of Content

List of Figures & Tables:

Chapter 1: Introduction

The evolution of technology and the consumerization of information have introduced new challenges in the data processing environment that can affect companies' share prices and shake public confidence in the nation's financial systems if not address. These challenges manifest themselves in the form of network vulnerabilities, data privacy issues, and identity theft to name a few. Greedy individuals and organizations alike have taken advantage of these technology related flaws and make millions at the expense of others. To mitigate/remediate these exposures, the government and the private sector have introduced new regulations and new mandates that companies must comply with. Complying with these regulations and mandates has introduced new cost challenges for companies as well. Companies have found themselves building multiple costly frameworks to address these regulations and mandates. The maintenance cost associated to these frameworks is astronomical.

Background/History

The evolution of technology has contributed tremendously to the tumbling down of various frontiers/barriers that once kept one corner of the world isolated from another. The journey that has led us to this juncture started long ago. A series of events have converged almost perfectly to turn the world into a virtual sandbox where everyone can work collectively. The core network architecture has changed from being a localized, stand-alone computing environment to a distributed environment where by, data lives on servers, workstations and other types of computing devices. Information travels through wires and airways at a rate that was not even conceived of 10 to 15 years ago.

The consumerization of information technology through such media as the internet, intranet, extranet (business partners' networks), and telecommunication not only make data protection complex, they make it extremely critical. Today, a majority of organizations could not function if they were to lose their computers and computing capabilities. Computers have been integrated into the business and individual daily fabric and their sudden unavailability would cause great pain and disruption. Many of the larger corporations already realize that their data is as much an asset to be protected as their physical buildings, factory equipment, and other physical assets. As computing and processing were brought closer to the people, the individuals who used computers learned more about using the technology and getting the most out of it. However, the good things in life often have a darker side.

Bringing technology down from the pedestal of the mainframe "glass house" into so many individuals' hands brought a lot of issues that never had to be dealt with in the mainframe days. Now there are thousands of people well versed and experienced in computing who have much more access to important data and processes. In the 1950s, the mainframe came into limited use in the government and

to coordinate communications security efforts, the government established the Communications Security Board. This was the first information security organization in the United States. The 1970s were a busy time in the computer security discipline. This era was characterized by a computing environment that is almost foreign to many users today. During this decade, the Department of Defense (DoD) undertook several computer security initiatives. The most important was DoD Directive 5200.28, which mandated the protection of classified information in DoD computer systems. This directive remained in effect until 2002. The Mitre Corporation developed an initial set of computer security evaluation criteria. These criteria were published in a document titled "Proposed Technical Evaluation Criteria for Trusted Computer Systems."

During the last couple decades, information/data protection took on more international importance, particularly in the face of the September 11th attacks, the Enron and WorldCom scandals which cost investors billions - witness the Sarbanes Oxley Act, privacy requirements based on the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) mandates, Customer Proprietary Network Information (CPNI) regulation, Personal Identifiable Information (PII) regulation, and increased oversight from other agencies.

Publicly traded businesses found themselves struggling to keep up with the virtual alphabet soup of compliance requirements. According to the results of a new web poll released by the Computing Technology Industry Association (CompTIA), data protection and security are swiftly becoming the biggest challenges for information technology (IT) professionals. As daunting as this might be, there is a powerful upside: companies now have an added incentive to improve business performance as they meet tighter compliance requirements.

The risks of noncompliance are real and tangible, from significant financial penalties to the threat of damage to an organization's reputation. Compounding the problem is the fact that the number of compliance regulations is growing; by some estimates, organizations will face twice as many compliance requirements by 2012 as they do today. The challenges of information security are constantly changing, often with those in the "bad actor" community able to operate with stealth, to share information about evolving technology and vulnerabilities, and to avoid prosecution by exploiting the differences in national approaches to cyber crime. Data privacy breaches, disruptive and fast spreading computer viruses/worms, consumerization of information technology, government regulations, and industry mandates have caused information security professionals endless angst. Companies have struggled to build costly and ineffective models to remain in compliance each time a new regulation or a new vulnerability surfaces.

Minimizing exposure, threat, and vulnerability associated with data leaks, un-hardened network environment, and un-safe software is rapidly becoming an essential line item in every business' objectives. One of the most effective ways to minimize business exposure is via an integrated framework that spans the entire IT fabric and aligns with business practices and priorities, as well as overall corporate policy. Information security controls, access controls, application controls, and system controls should be an integral part of every businesses' architecture "DNA". The novelty is that these controls apply not just to information technology issues but to management of all information that flows across an enterprise, along with its relations with customers, suppliers and partners.

Purpose

In the face of increasing requirements and expectations for continuous compliance, it is essential for compliance initiatives to be strategic, integrated business processes, and not one time projects. Answers must come from stakeholders understanding their respective roles and working towards common goals, so that enterprise systems are hardened to withstand attack and minimize exposure. A robust, systemic, and well architected "Integrated Compliance Framework for Data Processing Applications" that leverages industry best practices like the Control Objectives for Information and related Technology (COBIT), the Information Technology Infrastructure Library (ITIL), the International Organization for Standardization (ISO 27001/17799), the Capability Maturity Model (CMM), etc. must be implemented to enable companies doing business in this ever changing environment to take full advantage of their information, processes, and resources while ensuring integrity and availability of information technology systems and applications.

This research was done with the intention of identifying the major components necessary to assemble an integrated compliance framework and present practices that:

- Facilitate deployment in different data processing applications' setups
- Minimize the effort of complying with multiple, often overlapping compliance requirements
- Enable comprehensive visibility into an organization's infrastructure at the granular level
- Facilitate periodic audits to determine the adequacy and effectiveness of established controls, processes and procedures.

Chapter 2: Literature Review

Major Components of the Compliance Framework

Assembling the "Integrated Compliance Framework for Data Processing Applications" requires a working knowledge of the various regulations and industry mandates that data processing applications have to comply with. The critical components of the framework listed in "Figure 1 – Framework Components" were selected for their importance in maintaining a compliant environment.

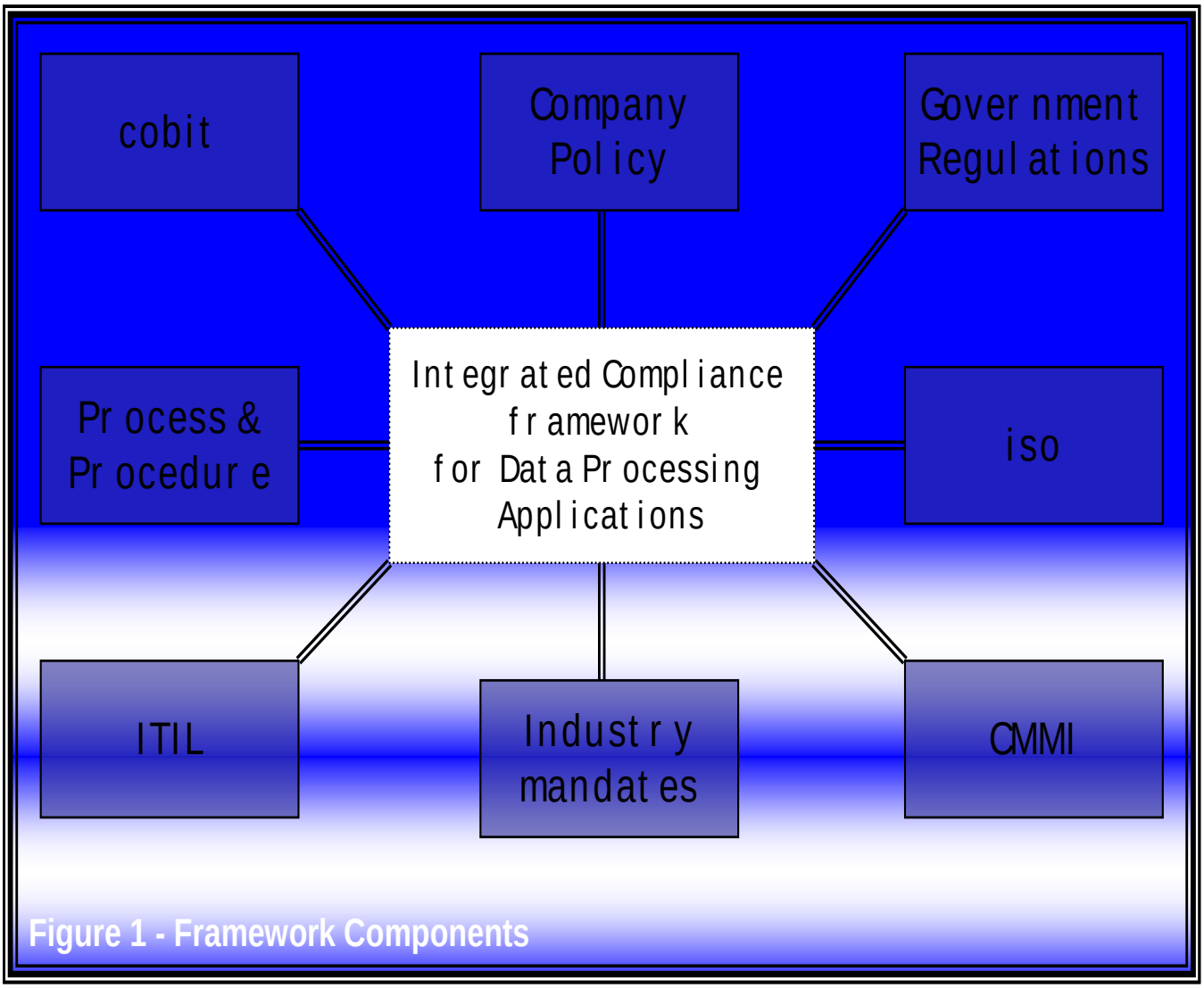


Figure 1 - Framework Components

Government Regulations

- **Sarbanes-Oxley Act of 2002 (SOX)**

  The Sarbanes-Oxley corporate governance act of 2002 is one of the biggest expansions of government regulation in 70 plus years. Also known as the Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called Sarbanes-Oxley, Sarbox, or SOX, the written law is a United States federal law enacted on July 30, 2002, as a reaction to a number of major corporate and accounting scandals including those affecting Enron and WorldCom. These scandals, which cost investors billions of dollars when the share prices of affected companies collapsed, shook public confidence in the nation's securities markets. Named after sponsors U.S. Senator Paul Sarbanes and U.S. Representative Michael G. Oxley, the act was approved by the House by a vote of 334-90 and by the Senate 99-0. President George W. Bush signed it into law, stating it included "the most far-reaching reforms of American business practices since the time of Franklin D. Roosevelt. (Bumiller)". The legislation set new or enhanced standards for all U.S. public company boards, management and public accounting firms. It does not apply to privately held companies. The act contains 11 titles, ranging from additional corporate board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law. The written law establishes stringent financial reporting requirements for companies doing business in the United States. It requires publicly held companies to implement internal controls over their financial reporting, operations and assets, to evaluate the strengths and weaknesses of these internal controls in official documents filed with the SEC and to make regular disclosures concerning the viability of these controls and potential fraud or losses that may affect the company's financial position.

  Debate continues over the perceived benefits and costs of SOX. Supporters contend the legislation was necessary and has played a useful role in restoring public confidence in the nation's capital markets by, among other things, strengthening corporate accounting controls. Opponents of the bill claim it has reduced America's international competitive edge against foreign financial service providers, saying SOX has introduced an overly complex regulatory environment into U.S. financial markets. According to a study done by Mckinsey & Company, the average public company devotes 30,000 plus man hours a year to support this Act. Several major companies are struggling to remain in compliance with this Act. The high cost of complying with the Act has to do with companies implementing new policies, procedures, standards, and processes that were not in existence before. These costs do impact their bottom line and they have to find a way to explain it to their shareholders.

- **Customer Proprietary Network Information (CPNI)**

  In the United States, Customer Proprietary Network Information (CPNI) is information that telecommunication services such as local, long distance, and wireless telephone companies acquire about their subscribers. It includes not only what services they use but their amount and type of usage. The Telecommunications Act of 1996 together with clarifications from the Federal Communications Commission (FCC) generally prohibits the use of that information without customer permission, even for the purpose of marketing to the customers other services. In the case of customers who switch to other service providers, the original service provider is prohibited from using the information to try to get the customer back. CPNI includes such information as optional services subscribed to, current charges, directory assistance charges, usage data, and calling patterns.

- **Health Insurance Portability and Accountability (HIPAA)**

  The Health Insurance Portability and Accountability Act (HIPAA) of 1996 mandates significant changes in the legal and regulatory environments governing the provision of health benefits, the delivery and payment of healthcare services, and the security and confidentiality of individually identifiable, protected health information.

  Failure to comply with any of the electronic data, security or privacy standards can result in civil monetary penalties up to $25,000 per standard per year. Violation of the privacy regulations for commercial or malicious purposes can result in criminal penalties of $50,000 to $250,000 in fines and one to ten years of imprisonment. The Civil Rights Division of the Department of Health and Human Services (DHHS) is charged with enforcement and is recognized as a stringent "enforcer." Providers who fail to comply also run the risk of violating public trust which can have untold public relations impacts.

- **Personally Identifiable Information (PII)**

  Personally Identifiable Information (PII) is data used to uniquely identify, contact or locate a person, including name, social security number, address, telephone number, email address, biometric records driver’s license number, vehicle registration plate, digital identity, etc. Although the concept of PII is ancient, it has become much more important as information technology and the internet have made it easier to collect PII, leading to a profitable market in collecting and reselling PII. The United States Senate has recently proposed the Privacy Act of 2005, which attempts to strictly limit the display, purchase, or sale of PII without the person's consent. Similarly, the Anti-phishing Act of 2005 attempts to prevent the acquiring of PII through phishing.

Industry Mandates

- **Payment Card Industry Mandate**

  The Payment Card Industry Security Standard (PCI DSS) is a common set of clear and concise security standards for processing, storing, or transmitting credit card numbers. It consists of the five major credit card brands:

  1) Visa
  2) MasterCard
  3) American Express
  4) Discover Card
  5) JCB International

  The PCI DSS began with each credit card issuer establishing their own proprietary programs to store and secure credit card data. Merchant concerns and confusion concerning rival and intersecting card brand-specific requirements, along with the continuation of massive credit card data breaches at many high profile organizations, prompted the card issuers to come together to create a single standard for protecting credit card data. In June 2005, American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International founded the PCI Security Standards Council (PCI SSC). The main tasks of the council are:

  - ✓ Creating, owning and managing PCI DSS for credit card data
  - ✓ Classifying a common audit requirement to certify compliance
  - ✓ Overseeing a certification process for security assessors and network scanning vendors
  - ✓ Instituting minimum qualification requirements
  - ✓ Retaining and publishing a list of certified assessors and vendors

  Under the PCI DSS, a business or organization should be able to assure their customers that its credit card data/account information and transaction information is safe from hackers or any malicious system intrusion. With data being stored virtually, in accessible areas, PCI standards are set up to help businesses with better practices. PCI DSS applies to every organization that processes credit or debit card information, including merchants and third-party service providers that store, process or transmit credit card/debit card data. These merchants must comply with the PCI Data Security Standard. However, according to the PCI DSS documentation, "PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply." The major credit card

companies have set strong incentives for banks to ensure their merchants and service providers achieve and maintain PCI compliance. In the event a breach of cardholder information occurs, any non-PCI compliant organization will suffer extremely damaging direct penalties handed down from these banks including, but not limited to:

- ✓ Fines up to $500,000 per incident
- ✓ Loss of right to accept credit cards
- ✓ Responsibility of all financial losses that result from the breach
- ✓ Responsibilities can include theft, fraud, card replacement, etc.

Capability Maturity Model (CMM)

The *Capability Maturity Model (CMM)* describes procedures, principles, and practices that underlie software development process maturity. This model was developed to help software vendors improve their development processes by providing an evolutionary path from an ad hoc, "fly by the seat of your pants" approach to a more disciplined and repeatable approach that improves software quality, reduces the life cycle of development, provides better project management capabilities, allows for milestones to be created and met in a timely manner, and takes a more proactive approach versus the less effective reactive approach. This model provides policies, procedures, guidelines, and best practices to allow an organization to develop a standardized approach to software development that can be used across many different groups. The goal is to continue to review and improve upon the processes to optimize output, increase capabilities, and provide higher quality software at a lower cost. The model provides a layered framework that allows different organizations the ability to implement continuous improvement. It is a tool for the software development company and a tool for those wanting to assess a vendor's development consistency and quality. Thus, if a (hypothetical) company JayhawksRUs wants a (hypothetical) software developing company, SoftwareRUs, to develop an application for them, they can choose to buy into the sales hype about how wonderful SoftwareRUs is, or they can ask for the company to be evaluated against the CMM model. Third-party companies evaluate software development companies to certify the organizations' product development processes. Many software companies have this evaluation done so they can use this as a selling point to attract new customers. There are five maturity levels defined:

- ✓ **Initial -** Development process is ad hoc or even chaotic. The company does not use effective management procedures and plans. There is no assurance of consistency, and quality is unpredictable.

- ✓ **Repeatable -** A formal management structure, change control, and quality assurance is in place. The company can properly repeat processes throughout each project. The company does not have formal process models defined.
- ✓ **Defined -** Formal procedures are in place that outline and define processes that are carried out in each project. The organization has a way to allow for quantitative process improvement.
- ✓ **Managed -** The company has formal processes in place to collect and analyze qualitative data, and metrics are defined and fed into the process improvement program.
- ✓ **Optimizing -** The company has budgeted and integrated plans for continuous process improvement.

At maturity level 5 (Optimizing), processes are concerned with addressing statistical common causes of process variation and changing the process to improve process performance. This would be done at the same time as maintaining the likelihood of achieving the established quantitative process-improvement objectives.

Information Technology Infrastructure Library (ITIL)

ITIL provides a systematic approach to the management of information technology service provision. It is the only consistent and comprehensive documentation of best practice for information technology service management. The Information Technology Infrastructure Library was originally created by the United Kingdom Government, but is now used throughout the world. The ethos behind the development of ITIL is the recognition that organizations are becoming increasingly dependent on IT in order to satisfy their corporate aims and meet their business needs. This leads to an increased requirement for high quality IT services. The most recent version of ITIL (v3) is comprised of five core texts known as Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement. There are several benefits for using the Information Technology Infrastructure Library for many IT business needs, and one main benefit is that, through the guidelines and best practices that are taught in the library, businesses can save a tremendous amount of money once implemented. Another advantage of ITIL is that it helps IT departments organize and manage many different disciplines using one comprehensive volume. ITIL is the leader in IT guidelines and best practice publications; it has been tested in real world environments for over a decade. Other advantages for adopting its guidance include:

- ✓ Improved information technology services through the use of proven best practice processes
- ✓ Improved customer satisfaction through a more professional approach to service delivery

- ✓ Standards and guidance
- ✓ Improved productivity
- ✓ Improved use of skills and experience
- ✓ Improved delivery of third party services through the specification of ITIL or ISO 20000 as the standards for service delivery in service procurements

International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is the world's largest developer and publisher of International Standards. It is a network of the national standards institutes of 162 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations. Therefore, ISO enables a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society.

ISO launches the development of new standards in response to sectors and stakeholders that express a clearly established need for them. An industry sector or other stakeholder groups typically communicate their requirement for a standard to one of ISO's national members. They later propose the new work item to the relevant ISO technical committee developing standards in that area. New work items may also be proposed by organizations in liaison with such committees. When work items do not relate to existing committees, proposals may also be made by ISO members to set up new technical committees to cover new fields of activity. To be accepted for development, a proposed work item must receive the majority support of the participating members of the ISO technical committee which, amongst other criteria, verifies the "global relevance" of the proposed item – this means that it indeed responds to an international need and will eventually be suitable for implementation on as broad a basis as possible worldwide. International Standards are developed by ISO technical committees (TC) and subcommittees (SC) using a six-step process:

- ✓ Stage 1: Proposal stage
- ✓ Stage 2: Preparatory stage
- ✓ Stage 3: Committee stage
- ✓ Stage 4: Enquiry stage
- ✓ Stage 5: Approval stage

- ✓ Stage 6: Publication stage

The committees and subcommittees provide technological, economic and societal benefits for businesses, innovators, customers, governments, trade officials, developing countries, consumers, etc. In order words, ISO standards:

- ✓ Make the development, manufacturing and supply of products and services more efficient, safer and cleaner
- ✓ Facilitate trade between countries and make it fairer
- ✓ Provide governments with a technical base for health, safety and environmental legislation, and conformity assessment
- ✓ Share technological advances and good management practice
- ✓ Disseminate innovation
- ✓ Safeguard consumers, and users in general, of products and services
- ✓ Make life simpler by providing solutions to common problems

ISO has developed over 17,500 international standards on a variety of subjects and some 1100 new ISO standards are published every year. Standards are classified according to the International Classification for Standards (ICS) and by Technical Committee (TC). The standards (see next page, "Table 1 – Critical Standards Impacted Data Processing") that are of interest in this research are the ones focusing on information technology developed by the subcommittees.

Table 1 – Critical Standards Impacted Data Processing	
Subcommittee	**Subcommittee Title**
JTC 1/SC 2	Coded character sets
JTC 1/SC 6	Telecommunications and information exchange between systems
JTC 1/SC 7	Software and systems engineering
JTC 1/SC 17	Cards and personal identification
JTC 1/SC 22	Programming languages, their environments and system software interfaces
JTC 1/SC 23	Digitally Recorded Media for Information Interchange and Storage
JTC 1/SC 24	Computer graphics, image processing and environmental data representation
JTC 1/SC 25	Interconnection of information technology equipment
JTC 1/SC 27	IT Security techniques
JTC 1/SC 28	Office equipment
JTC 1/SC 29	Coding of audio, picture, multimedia and hypermedia information
JTC 1/SC 31	Automatic identification and data capture techniques
JTC 1/SC 32	Data management and interchange
JTC 1/SC 34	Document description and processing languages
JTC 1/SC 35	User interfaces
JTC 1/SC 36	Information technology for learning, education and training
JTC 1/SC 37	Biometrics

Control Objectives for Information and related Technology (COBIT)

The *Control Objectives for Information and related Technology* (COBIT) is a framework and supporting tool set that allow managers to bridge the gap with respect to control requirements, technical issues and business risks, and communicate that level of control to stakeholders. It is based on the analysis and harmonization of existing IT standards and good practices and conforms to generally accepted governance principles. COBIT enables the development of clear policies and good practice for information technology control throughout enterprises. COBIT has become the integrator for information technology good practices and the umbrella framework for IT governance that helps in

understanding and managing the risks and benefits associated with information technology. The process structure of COBIT and its high-level business-focused, process-oriented, controls-based, and measurement-driven approach provide an end-to-end view of IT and the decisions to be made about IT. The benefits of implementing COBIT as a governance framework over IT include:

- ✓ Better alignment, based on a business focus
- ✓ A view, understandable to management, of what IT does
- ✓ Clear ownership and responsibilities, based on process orientation
- ✓ General acceptability with third parties and regulators
- ✓ Shared understanding amongst all stakeholders, based on a common language
- ✓ Fulfillment of the Committee of Sponsoring Organizations (COSO) requirements for the IT control environment

Data Processing Policy, Process, and Procedure

Data processing policies, processes, and procedures are essentials in a company overall strategy. If suitable, sufficient, and consistently applied, they enable companies to conduct business at reduced risk while taking full advantage of their information, processes, and resources. The policy dictates the processes, procedures, business needs, laws, regulations, and standards of due care that a company must adhere to. It is directed, driven, and supported by senior management.

Texts & Webinars Review

Managing Projects in Organizations (Frame)

The book presents project management as the application of knowledge, skills, tools and techniques applied to a broad range of activities to achieve a stated objective, such as meeting the defined user requirements and deadlines for a design & build or an information systems project. According to the author, project management knowledge and practices are best described in terms of their component processes of initiating, planning, executing, controlling, and closing projects. Overall characteristics of successful project planning are that it is a risk-based management process and iterative in nature.

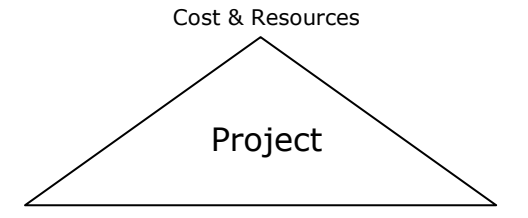


Figure 2 – Project Management Triangle

Project management techniques also provide systematic quantitative and qualitative approaches to project size estimating, scheduling, allocating resources and measuring productivity. There are

numerous project management techniques and tools available to assist the project manager in controlling the time and resources utilized in the development of a system, design, etc. They may vary from a simple manual effort to a more elaborate computerized process. The size and complexity of the project may require different approaches.

There are three elements or dimensions of a project depicted in "Figure 2 - Project Management Triangle" that should always be taken into account. The figure depicts the relationship among the three elements. From a heuristic view, the area of the triangle surrounding the project remains constant but the length of the sides may vary. The behavior of the triangle greatly depends on its degree of freedom. If, for example constraints exist in two dimensions, the remaining side is automatically determined. If there is only one constraint, then one dimension can be freely chosen and the last dimension has to compensate. An important element of the deliverables that is also considered during the management of time and resources is the quality of the deliverables. The parameters for quality of the deliverables may be specified clearly by the project steering committee or project sponsor, or the project manager may have to elicit this from user management. In either case, the project manager must have a clear and documented view of the quality expectation for the deliverables from the project steering committee, sponsor, and users.

The complexity of project management requires a careful and explicit design of the project management process, as normally done for a business process but often neglected for the project management process. Thus, all design issues applicable for business process engineering should also be applied for the project management process. Projects that must comply with laws and regulations require more up-front planning. When project managers consider the regulations that govern their industry, from manufacturing to health care, the regulations become project constraints and result in more overhead. Factoring laws and regulations into projects also expands their scope and adds to their costs. PMs have to become fluent with these ever changing regulations and industry mandates in order to deliver high quality products on schedule that meet customers' expectations.

The Sarbanes-Oxley Guide for Finance & IT Professionals (Anand)

This book provides an in-depth review of the various components/sections of the Sarbanes-Oxley Act which was enacted after the Enron and WorldCom debacles and in response to the resulting dramatic loss of faith in the government of public companies. It discusses the main objectives of the Act and presents some solid frameworks to begin, or build on, the task of corporate compliance. The Act is built on integrity, independence, proper oversight, accountability, strong internal controls, transparency, and deterrence. While the Sarbanes-Oxley Act of 2002 covers 11 titled components and consists of 66

Sections; the author presents Section 302 which deals with disclosure controls and procedures, and Section 404 which addresses internal controls and procedures as the two Sections that are getting the most publicity and pose the greatest challenge to implement.

The certification process identified in Section 302 and implemented by the Security and Exchange Commission (SEC) requires the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) to personally certify that the corporate reports that they are filing with the SEC are accurate and complete. Section 404 requires the company to disclose the effectiveness of its internal control systems by outlining management's responsibilities for maintaining an adequate control system and assessing the system's performance at the end of each fiscal year. Though these Sections work in unison to ensure that financial information is reported accurately, the cost of implementing the supporting controls is astronomical. The average public company normally devotes 30,000 man hours a year on average to support this Act. Several major companies are struggling to remain in compliance with this Act. The high cost of complying with the Act mostly comes from the implementation of new policies, procedures, standards, and processes that were not in existence before. Failure to comply with the Sarbanes-Oxley Act of 2002 may result in fine up $5,000,000 and/or imprisonment of up to 20 years.

IT Compliance & Controls - Best Practices for Implementation **by James J. Deuccia**

In this book the author provides an in-depth review of Information Technology (IT) internal controls and answers the question, "How much is enough?" Along with providing protection for their organizations, Chief Information Officer (CIO) and Chief Technology Officer (CTO) need to address compliance issues identifying appropriate controls and its relationship with the global market. Recent awareness of the importance of technology by key stakeholders has raised the visibility and scrutiny placed upon the safeguards employed in organizations. No longer may technology be considered after the fact, but must be evaluated prudently at the highest levels to consider the full impact of security, resiliency to operations, integrity of services, propriety of partnerships with vendors, and the inevitable risks of operating any business.

The author presents field-tested ideas forged from the fires of direct experience with clients who are daily hammering out their technology to become competitive business models and lays a foundation by examining the importance of internal IT controls defining US government oversight measures. Furthermore, the author explains why silo IT strategy wastes time and resources, offering a better solution in having an IT enterprise control environment. In the third section of the book, the author takes a practical approach to evaluating the organization's IT internal controls needs and merges these with the regulated mandates as he develops a plan to achieving a balance of business and assurance. "IT

Compliance and Controls" includes a thorough breakdown of a core set of principles and showing readers how to implement these best practices successfully. It provides proven, systematic approaches to map IT controls directly to specific regulatory requirements such as the SAS70, Sarbanes Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), European Union (EU) Directives, etc. The book reveals the globalization of internal controls, and why this interconnected world must be understood, acknowledged, and embraced universally.

Law, Investigation and Ethics Objectives Webinar by Brightalk

This is one of a number of modules that were presented by Brightpoint around computer security. This module focused mainly on types of computer crimes, privacy issues, and investigation of computer crimes. In the webinar, computer and associated information crimes were portrayed as natural response of criminals to society's increasing use of and dependence on technology. However, crime has always taken place, with or without a computer. A computer is just another tool and, like other tools before it, it can be used for good or evil. Fraud, theft, and embezzlement have always been part of life, but the computer age has brought new opportunities for thieves. A new degree of complexity has been added to accounting, record keeping, communications, and funds transfer. This degree of complexity brings along its own set of vulnerabilities, which many thieves are all too eager to take advantage of. Companies are being blackmailed by cybercriminals who discover vulnerabilities in their networks. Company trade secrets and confidential information are being stolen when security breaches take place. Online banks are seeing a rise in fraud, and retailers' databases are being attacked and robbed of their credit card information. More and more companies are losing money in profits and productivity because of the rise in denial-of-service (DoS) attacks. As e-commerce and online business become enmeshed in today's business world, these types of issues become more important and more dangerous. Hacking and attacks are continually on the rise, and companies are well aware of it. The legal system and law enforcement seem to be behind in their efforts to track down cybercriminals and successfully prosecute them. New technologies to fight many types of attacks are on the way, but a great need still exists for proper laws, policies, and methods of actually catching the perpetrators and making them pay for the damage they cause.

Many companies are doing business across state lines and in different countries. This brings even more challenges when it comes to who has to follow what laws. Different states can interpret the same law differently. One country may not consider some issues against the law at all, whereas another country may determine that the same issue demands five years in prison. One of the complexities in these issues is jurisdiction. If a thief from another country steals a bunch of credit card numbers from an American financial institution and he is caught, a court in America would want to prosecute him. His homeland

may not see this issue as illegal at all. Although the attackers are not restricted or hampered by country borders, the laws are in many cases. Despite all this confusion, there are some clear-cut responsibilities that companies have pertaining to computer security issues and specifics on how companies are expected to prevent, detect and report crimes.

Applications and System Development Objectives Webinar by Brightalk

This is one of a number of modules that were presented by Brightpoint around compliance. This module focused mainly on software flaws, database concepts and security issues, software lifecycle development processes, change control concepts, and object-oriented programming components. According to the presenter, applications and computer systems are usually developed for functionality first, not security first. To get the best of both worlds, security and functionality would have to be designed and developed at the same time. Security should be interwoven into the core of a product and provide protection at different layers; this is a better approach than trying to develop a front end or wrapper that may reduce the overall functionality and leave security holes when the product has to be integrated with other applications. The discussion veered into the several types of models that are in used for system or application development and the core components that are common to all of them. Each model basically accomplishes the same thing; the main difference is how the development and lifecycle of a system is broken into sections. A project can start with a good idea, and then the programmers and engineers just wing it, or the project can be carefully thought out and structured to follow the necessary life cycles. The first option may seem more appropriate in the beginning because open ended requirements and steps can be skipped, documentation can be overlooked, and the product can be released in a shorter time and under budget. However, more fun would actually be had by the team that took its time to think through all of the scenarios of each phase of the life cycle because its product would be more sound, become more trustworthy by the market, the team would make more money in the long run, and it would not need to chaotically develop several service and security patches to fix problems missed the first time around. The different models integrate the following phases in one fashion or another:

- ✓ Project initiation
- ✓ Functional design analysis and planning
- ✓ System design specifications
- ✓ Software development
- ✓ Installation/implementation
- ✓ Operational/maintenance

As could be noticed, compliance is not listed as a bullet point that would indicate it is dealt with in one phase or another. This is because compliance should be embedded throughout all phases. It costs a lot more money to address security issues after the product is released compared with addressing it during the development of the product.

Summary

Institutionalizing compliance in the core components of a business model is rapidly becoming a critical element in a company's overall strategy. The benefit to be gained in implementing a compliance framework that harmonizes controls across the information technology industry far outweighs the cost associated with building such infrastructure. The challenges of information security have morphed into different type of vulnerabilities and exposures over time and they are rapidly multiplying. Data privacy breaches and disruptive/fast spreading computer viruses/worms are just a few headaches that companies doing business in this modern era have to deal with. In February 2005, ChoicePoint acknowledged that it had mistakenly sold personal information on thousands of individuals—as it turned out, more than 163,000 people—to bogus companies set up by Nigerian criminals. The Federal Trade Commission fined the Alpharetta, Ga.-based company $15 million for the disclosures and the company's stock lost 20% of its value in one day. Carol DiBattiste, ChoicePoint's chief credentialing, compliance and privacy officer, says the company has taken numerous steps to make sure such a breach never happens again.

An integrated framework undoubtedly reduces the cost associated with meeting compliance and security requirements effectively and efficiently. It also enables companies to conduct business at reduced risk while taking full advantage of their information, processes, and resources. Each component of the "Integrated Compliance Framework for Data Processing Applications" as described in previous sections plays a crucial role in addressing data security, vulnerability, and exposure. Such infrastructure facilitates the design of a program that affect long term changes not just remediating tactical gaps. This research focused mainly on compliance as it relates to data processing applications. A framework which addresses the following components were assembled and validated using data from a series of interviews conducted with data processing application SMEs (Subject Matter Experts), application developers, and business users:

- ✓ Policies, Processes, and Procedures
- ✓ Industry Mandates, Regulations, and Best practices
- ✓ Risk/Issue Management, Accountability Matrix, Integrated Compliance Architecture, and Applications Assessment Toolkit

Chapter 3: Research Procedure

This section of the report introduces the methodological approach used to gather the necessary data to assemble the "Integrated Compliance Framework for Data Processing Applications" which leverages multiple frameworks with different approaches to solving compliance problem to deliver a more comprehensive approach that tackles compliance from a regulatory, industry mandates, and company processes perspective. Information was gathered through researches, literature reviews, along with various discussions/meetings with Compliance Specialists, Methodologists, Project Managers, Software Engineers, and Requirement Managers with the quest to demystify the compliance model.

Data Collection

In order to insure a comprehensive review, a number of websites (Google, Yahoo, the Information Technology Infrastructure Library (ITIL) website, the Information Systems Audit and Control Association (ISACA) website, the International Organization for Standardization (ISO) website, and a few others that contain regulatory and industry mandates data) and books as outlined in the literature review section of this report were utilized. While it was fairly easy to locate books, websites, and articles on the regulations, industry mandates, project management, and compliance frameworks, it was not as simple to find artifacts on the integration of software development methodologies with compliance framework.

For the "original thought" portion of this field project and to develop the "complete" integrated framework, peer inputs and personal experience were relied on. A quick survey was assembled (see next page, Table 2 - Compliance Questionnaire) which was distributed via email to 23 Project Managers (PM) and 15 Requirement Managers (RM) to get their point of views on the need for an integrated compliance model/framework in the data processing environment. This population comprises of PM and RM throughout the information technology industry.

Compliance Questionnaire	
#	Question
1.	Have you worked on projects that are impacted by regulations or industry mandates since performing this job?
2.	Are you required to complete compliance training in order to perform this job?
3.	Do you know the various regulations and industry mandates that may impacts your projects?
4.	Does the business community you support know of the various regulations and industry mandates that may impacts your projects?
5.	Is the compliance function centralized in your company?
6.	Is there a quality assurance/compliance/security resource assigned to each and every project you have worked on?
7.	Does the methodology that you use to deliver products contain quality assurance/compliance gate reviews?
8.	Do you ever have to change project schedule/cost due to security, regulatory, and/or industry mandate issues that you did not plan for?
9.	Is upper management enforcing compliance in your organization?
10.	Do you know the importance of compliance in the organization?

Table 2 - Compliance Questionnaire

Process/Framework Analysis

A number of frameworks from the internet and other places pertaining to compliance with regulations, internal processes, and contractual agreement were collected and reviewed. The fundamental differences were mainly in their approach to delivery and implementation cost, their core components were very similar conceptually. The frameworks supporting the Payment Card Industry mandates call for the implementation of an infrastructure that facilitates compliance with PCI, the frameworks supporting the Sarbanes-Oxley Act of 2002 call for the implementation of an infrastructure that facilitates compliance with the act, those supporting data privacy call for the implementation of an infrastructure that facilitates compliance with the data privacy regulations.

Given the current model, a publicly traded company that processes credit card data would have to implement and maintain at least three frameworks in order to comply with PCI mandates, SOX and data privacy regulations. These businesses, in many cases, will build costly and ineffective models just to remain in compliance each time a new regulation, a new industry mandate, or a new vulnerability surfaces.

Cost/Benefit Analysis

According to an article written by CIOInsight, ChoicePoint mistakenly sold personal information on 163,000 people to bogus companies set up by Nigerian criminals and was fined $15M by the Federal Trade Commission. In addition the company's stock lost 20% of its value on the day the news was released.

CanWest News Service wrote in article published in March 2007, TJX, the parent company for discount clothing stores T.J. Maxx, Marshalls and some others had lost some 455, 000 credit cardholders' data after their systems were hacked (data leak) back in 2006. They had paid an undisclosed amount in fine.

The Enron and WorldCom scandals which cost investors billions of dollars when the share prices of affected companies collapsed. Though, Enron and WorldCom both went under, these scandals shook public confidence in the nation's securities markets.

Compliance is not inexpensive. In many cases, the high cost of complying with regulations and industry mandates has to do with companies implementing new processes/frameworks to address regulations, industry mandates, and vulnerabilities as they surface. An integrated framework undoubtedly should reduce the cost associated with meeting compliance and security requirements effectively and efficiently.

Several projects pulled from an internal project repository were reviewed and a number of compliance related defects/vulnerabilities in the production environment were found related to some of these projects. The cost of fixing these vulnerabilities after the fact is only a fraction of what it would have cost to address the compliance requirements early on. The benefit to be gained in implementing a robust, systemic, integrated, and well architected compliance framework far outweighs the cost associated to building and maintaining it.

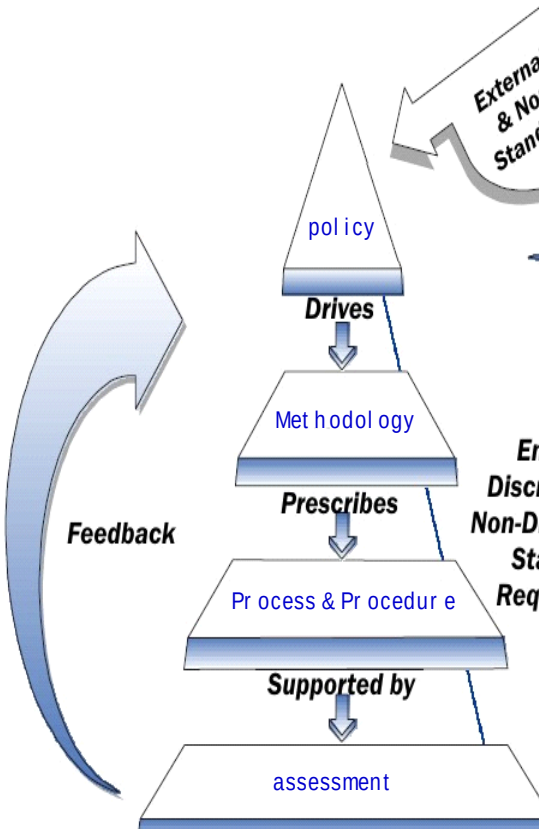
Packaging

The research topic and approach were vetted with a few Compliance Specialists, Solutions Architects, Methodologists, Project Managers, Software Engineers, and Requirement Managers throughout the data processing industry and the feedback that was received thus far is very encouraging. The final product will be made available to these resources for review and hopefully they will provide additional feedback to further improve the quality of such framework.

Chapter 4: Framework

Integrated Compliance Architecture

Computers and the information that is processed on them usually have a direct relationship with a company's critical missions and objectives. Because of this level of importance, senior management should make protecting these items a high priority and provide the necessary support, funds, time, and resources to ensure that systems, networks, and information are protected in the most logical and cost-effective manner possible.



Data Processing - Policy

A cornerstone in the foundation of the supporting infrastructure for the "*Integrated Compliance Framework for Data Processing Applications*" is an un-ambiguous and robust policy which sets the tone for the compliance program throughout an organization. The policy states management's intent pertaining to how compliance should be practiced within an organization, what actions are acceptable, and what level of risk the company is willing to accept. The policy is derived from the laws, regulations, and business objectives that shape and restrict the company. Furthermore, it provides direction for each employee and department regarding how compliance should be implemented and followed, and the repercussions for non-compliance. The policy includes, but not limited to, the following core components which are the foundation for a successful compliance program:

- ✓ Executive Summary

  The policy's executive summary should be clear and concise. It should summarize the significant components of the policy and set the tone for how the entire document is to be decoded and adhered to. The document should be signed by the executive with the highest authority in the company.

- ✓ Information Systems Development

  Information System Development (ISD) is an overall architecture (methodology) that supports project management through the product development lifecycle. It embodies an analytical framework which is conveyed through inter subjective representational practices and operationalized through a 'toolbox' of analytical methods, tools and techniques. The standardization of organizational procedures is critical to the definition of the ISD methodology so that development outputs may conform to pre-defined standards, and pre-defined expectations. Underlying all of these elements is a philosophical basis, which justifies the need for each element of the methodology and ensures inter subjectivity and commitment between development team members. The elements of an ISD methodology may vary from company to company. However, the fundamental - analyze, design, build, and deploy - remains the same.

- ✓ Information Systems Change Control

  Information System Change Control (ISCC) is the methodology used to manage change, configuration, and incident in a production environment. It provides a common framework of tasks, deliverables, and milestones required to be completed during execution. The changes can happen to network configurations, system parameters, applications, and settings when adding new technologies, application configurations, or devices, or when modifying the facility's environmental systems. Change control is important not only for an environment, but also for a product during its development and life cycle. Changes must be effective and orderly, because time and money can be wasted by continually making changes that do not meet an ultimate goal. The change control component of the policy should indicate how changes take place within a facility, who can make the changes, how the changes are approved, and how the changes are documented and communicated to other employees. Without this component of the policy in place, people can make changes that others do not know about and that have not been approved, which can result in a confusing mess at the lowest end of the impact scale, and a complete breakdown of operations at the high end.

- ✓ Information Security

  The Information Security (IS) component dictates the processes governing the system environment. It provides details on how accesses to system components (application, database, operating system, server, etc.) are to be granted, revoked, and audited periodically. Ownership should be clearly defined and the user community of IS should include those involved in using,

implementing, and supporting the systems environment. Users' access to resources must be limited and properly controlled to ensure that excessive privileges do not provide the opportunity to cause damage to a company and its resources. Users' access attempts and activities while using a resource need to be properly monitored, audited, and logged. The individual user ID needs to be included in the audit logs to enforce individual responsibility. Each user should understand his responsibility when using company resources and be accountable for his actions.

- ✓ Information Systems Operations

  The Information Systems Operations (ISO) comprises of processes and procedures around computer support, backup/recovery, record retention, tape management, batch processing/job control security, and data security.

- ✓ Role & Responsibility

  In order to ensure the effectiveness of the compliance program through an organization and to uphold institutional commitment to compliance, the first step a board of directors and senior management should take in providing for the administration of a compliance program is the designation of a compliance officer, regardless of size or institution complexity. In developing the organizational structure of the compliance program, a board and senior management must grant a compliance officer sufficient authority and independence to cross departmental lines to access all areas of the institution's operations, and to effect corrective action. Leadership on compliance by the board of directors and senior management sets the tone in an organization. The board and senior management should discuss compliance topics during their meetings. They should include compliance matters in their communications to institution personnel and the general public. Institution management and staff should have a clear understanding that compliance is important to the board and senior management, and that they are expected to incorporate compliance in their daily operations. Compliance efforts require an ongoing commitment from all levels of management. The Chief Compliance Officer (CCO) is mainly responsible to lead the enterprise compliance efforts, designing and implementing internal controls, policies, processes, and procedures to assure compliance with applicable regulatory requirements, industry mandates, and third party guidelines; managing audits and investigations into regulatory and compliance issues; training management and employees in consumer protection laws and regulations and responding to requests for information from regulatory bodies.

To be effective at overseeing compliance and maintaining a strong compliance posture, a compliance officer must be provided with ongoing training, as well as sufficient time and adequate resources to do the job. The compliance officer may utilize third-party service providers or consultants to help administer the compliance program or audit functions. However, the compliance officer should perform sufficient due diligence to verify that the provider is qualified, because ultimately the institution is accountable for compliance with consumer protection laws and regulations.

✓ Accountability Matrix

AREA	SUB-AREA	RESPONSIBLE & ACCOUNTABLE	REVIEWER
INFORMATION SYSTEM DEVELOPMENT	Software Development Life Cycle (SDLC) methodology	?	?
	Vendor management methodology	?	?
	Risk and issue management methodology	?	?
INFORMATION SYSTEM CHANGE CONTROL	Application and general controls	?	?
INFORMATION SECURITY	Information Classification	?	?
	Access management	?	?
	Information Ownership	?	?
	Protection of data in transit and in storage	?	?
INFORMATION SYSTEM OPERATIONS	Protection of hardware & Software (computing systems)	?	?
	Security Incident Response	?	?
	Security monitoring and compliance Reviews	?	?
	Data Retention, backup and recovery		
TRAINING	Compliance training program.	?	?
ASSESSMENT/ AUDITING	Assessment/Auditing program.	?	?
QUALITY ASSURANCE	Monitoring	?	?
	Maintenance	?	?

Table 3 – Accountability Matrix

Data Processing – Processes and Procedures

As depicted in “Figure 3 – Integrated Compliance Architecture”, processes, procedures, standards, and guidelines which are prescribed by the methodology provide the details that support and enforce the

company's compliance policy. They should be maintained in a centralized location that is readily available to all resources in the enterprise and they should be tested on a periodic basis to ensure that they properly support the compliance policy, goals, and objectives set for them. The testing can be a drill to test reactions to a physical attack or disruption of the network, a penetration test of the firewalls and perimeter network to uncover vulnerabilities, a query to employees to gauge their knowledge, or a review of the procedures and standards to make sure they still align with business or technology changes that have been implemented. Because change is constant and environments continually evolve, compliance procedures and practices should be continually tested to ensure that they align with management's expectations and stay up to date with each addition to the infrastructure. It is management's responsibility to make sure these tests take place.

Data Processing – Methodology

From the 38 PMs and RMs surveyed, the majority of those that responded (32 out of 38) pointed out that they often find out about regulatory or industry impacts to their projects too late in the project development life cycle. In addition, they have never received any training on compliance nor do they know their role in enforcing it. A small number (5 out of 38) went through some level of compliance training but the training was not made mandatory to perform their current job function. Even more disappointing and alarming was the number (36 out of 38) of PMs and RMs that answered "NO" to item #3 (Do you know the various regulations and industry mandates that may impacts your projects?) in the questionnaire. These findings revealed that the need for the integrated compliance framework is an absolute necessity for data processing companies doing business in this ever changing environment.

The established methodology, dictated by the policy, should be the only channel through which hardware and software are acquired, developed, and/or maintained. This practice facilitates the process of ingraining compliance in the core systems (applications, database, operating systems, etc.) and minimizes risk. Throughout the industry, there are a number of methodologies (waterfall, agile, etc.) that are being used for development and/or procurement of software and hardware. Regardless of the Software Development Life Cycle (SDLC) methodology selected, compliance should be embedded throughout all phases. Most methodologies integrate analysis, design, build/test, implementation, and maintenance in one fashion or another. As depicted in "Figure 4 – Integrated SDLC Methodology and Compliance Framework", the two components (Methodology & Compliance) can be coalesced to minimize risks and exposure associated to a company's core systems. However, for the integration to be successful, senior management has to make it a priority as mentioned before to adopt and implement a robust compliance program that is driven by policy which in turn drives the methodology. Key stakeholders, Subject Matter Experts (SME), and project resources all have a critical role to play in

ensuring that artifacts/deliverables dictated by the integrated framework are produced and reviewed throughout the project lifecycle.

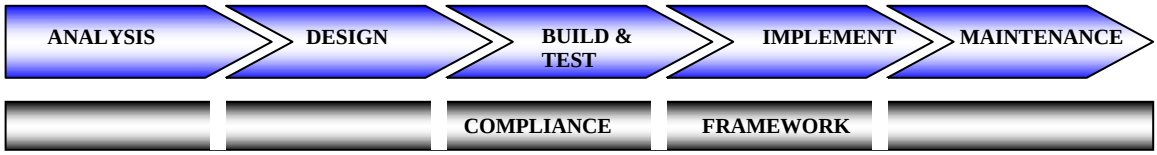


Figure 4 – Integrated SDLC Methodology & Compliance Framework

Analysis Phase & Compliance

This is the phase when everyone involved attempts to understand why the project is needed and what the scope of the project entails. Either a specific customer needs a new system or application, or there is a demand for the product in the market. At this point, the characteristics of the system and proposed functionality are discussed, brainstorming sessions take place, and obvious restrictions are reviewed. A conceptual definition of the project needs to be initiated and developed to ensure that everyone is on the right page and that this is a proper product to develop what will be, hopefully, profitable.

This phase could include evaluating products that are currently on the market and could identify any demands that are not being met by current vendors. It could also be a direct request for a specific product from a current or future customer. In either case, because this is for a specific client or market, an initial study of the product needs to be started, and a high-level proposal should be drafted that outlines the necessary resources for the project and the predicted timeline of development. The estimated profit expected from the product also needs to be conducted. This information is submitted to senior management who will determine if the next phase should begin or if further information is required.

In this phase, the user needs are identified and basic compliance objectives of the product are acknowledged. It must be determined if the product will be processing sensitive data, and if so, the levels of sensitivity involved should also be defined. An initial risk analysis should be initiated that evaluates threats and vulnerabilities to estimate the cost/benefit ratios of the different security countermeasures. Issues pertaining to security integrity, confidentiality, and availability need to be addressed. The level of each security attribute should be focused upon so that a clear direction of security controls can begin to take shape.

A basic security framework is designed for the project to follow, and risk management processes are established. Risk management will continue throughout the lifetime of the project. The first step in risk management is to identify the threats and vulnerabilities and to calculate the level of risk involved. It usually involves asking many, many questions to find out the laundry list of vulnerabilities and threats,

the probability of these vulnerabilities being exploited, and the outcome if one of these threats actually becomes real and a compromise takes place. The questions vary from product to product—its intended purpose, the expected environment it will be implemented into, the personnel involved, and the types of businesses that would purchase and use this type of product. A banking software product may need to be designed to have Web server farms within a network segment that is separated from other networks in the branch, but have the components and databases behind another set of firewalls to provide another layer of protection. This would mean that the architecture of the product would include splitting it among different systems and developing communication methods between the different parts. If the product is going to provide secure e-mail functionality, then all the risks involved with just this service need to be analyzed and properly accounted for. Implementation procedures need to be thought through and addressed. How will the customer set up this product? What are the system and environment requirements? Does this product need to be supplied with a public key infrastructure (PKI)? The level of maintenance required after installation is important to many products. Will the vendor need to keep the customer abreast of certain security issues? Should any logging and auditing take place? The more these things are thought through in the beginning, the less scrambling will be involved at the end of the process. When all the risks are evaluated, management will decide upon the acceptable level of risk. Of course, it would be nice for management to not accept any risks and for the product to be designed and tested until it is foolproof; however, this would cause the product to be in development for a long time and to be too expensive to purchase. Compromises and intelligent business decisions need to be made to provide a balance between risks and economic feasibility.

	TASK	OWNER
Analysis	Identify compliance requirements	Solutions Architect
	Perform compliance risk analysis	Solutions Architect & Requirement's Manager
	Identify project compliance framework	Solutions Architect
	Define compliance requirements	Solutions Architect & Requirement's Manager
	Implement compliance checkpoints in plan	Project Manager
	Generate preliminary compliance test plans	Project Manager, Requirement's Manager, and Solutions Architect
	Perform compliance gate reviews	Project Manager, Solutions Architect, & Quality Assurance Team
	Obtain approvals from stakeholders	Project Manager

Table 4 – Compliance Tasks - Analysis Phase

Design Phase & Compliance

In the design phase, compliance starts to take shape. Requirements gathered during the analysis phase drives the design. The design, in turn, addresses what mechanism is needed to provide the compliance functionality and determines how it will be coded, tested, and implemented. This is where high-level questions are asked. Examples of these questions include the following: Are authentication and authorization necessary? Is encryption needed? Will the product need to interface with other systems? Will the product be directly accessed via the Internet? Access control mechanisms are chosen, subject rights and permissions are defined, the encryption method and algorithm are chosen, the handling of sensitive data is ironed out, the necessary objects and components are identified, the inter processing communication is evaluated, the integrity mechanism is identified, and any other compliance specifications are appraised and solutions are determined. The modularity and reusability of the product or the components of the product are addressed. Code that provides security-critical functions should be simple in design in order to catch errors in a less confusing fashion, and be small enough to be fully tested in different situations. Compliance components can be called and used by different parts of the product or by other applications. This attribute, reusability, can help streamline the product and provide for a more efficient and more structured coding environment.

A robust project plan is assembled to define the compliance activities and to create compliance checkpoints to ensure that quality assurance for compliance controls takes place and that the configuration and change control process is identified. At this point in the project, resources are identified, test schedules start to form, and evaluation criteria are developed to be able to properly test the compliance controls. A formal functional baseline is formed, meaning the expectations of the product are outlined in a formal manner, usually through documentation. A test plan is developed, which will be updated through each phase to ensure that all controls are properly tested.

The initial risk assessment will most likely be updated throughout the project as more information is uncovered and learned. In some projects, more than one risk analysis needs to be performed at different stages of the life cycle. For example, if the project team knows that the product will need to identify and authenticate users in a domain setting requiring a medium level of security, an initial risk analysis is performed. Later in the life cycle, if it is determined that this product should work with biometric devices and have the capability to integrate with systems that require high security levels, a whole new risk analysis will need to be performed because new morsels have been added to the mix. This phase addresses the compliance functionality required out of the product and is captured in a design document. If the product is being developed for a customer, the design document is used as a tool to explain to the customer what the developing team understands of the requirements of the product. A design document

is usually drawn up by analysts, with the guidance of engineers and architects, and presented to the customer. The customer can then decide if more functionality needs to be added or subtracted, and dialogues between the customer and development team begin hammering out exactly what is expected from the product. Many companies either skip the functional design phase and start developing specifications for the product or don't share the design with the customer. This can cause major delays and rework efforts, because a broad vision of the product needs to be developed before looking strictly at the details. A lot of wasted time can go into developing a product that is not what is actually wanted by the customer, so clear direction and goals need to be drawn up before the beginning of coding. This is usually an important function of the project management team.

	TASK	OWNER
Design	Define compliance specifications	Solutions Architect & Project Manager
	Review & update compliance risk analysis	Solutions Architect & Project Manager
	Update test plans involving compliance	Solutions Architect, Test Engineer, and Project Manager
	Develop system design compliance checklist	Solutions Architect, Project Manager, & Test Engineer
	Perform compliance gate reviews	Project Manager, Solutions Architect, & Quality Assurance Team
	Obtain approvals from stakeholders	Project Manager

Table 5 – Compliance Tasks - Design Phase

Build/Test Phase & Compliance

This is the phase where compliance resources become deeply involved. Compliance components from the design are being integrated with the software or hardware that is being requested. Checking for buffer overflows, authentication parameters, encryption of sensitive data elements in an interface, business approvals of test cases, network segmentation, data protection, and data leakage are becoming real.

Different attack scenarios can be played out to see how the code or hardware could be attacked or modified in an unauthorized fashion. Formal and informal testing should begin as soon as possible. There is no cookie-cutter recipe for compliance testing, because the applications and products can be so diverse in functionality and compliance objectives. It is important to map compliance risks to test cases and code. Linear thinking can be followed by identifying a risk, providing the necessary test scenario, performing the test, and reviewing the code for how it deals with such a risk. At this phase, tests are conducted in an actual network, which should mirror the production environment to ensure the code does not only work in the labs. Security attacks and penetrations usually take place during this phase to identify any missed vulnerabilities. Functionality, performance, and penetration resistance are evaluated.

All the necessary functionality required of the product should be in a checklist to ensure that each one is accounted for.

Security tests should be run to test against the risks identified earlier within the project. Buffer overflows should be attempted, the product should be hacked and attacked, interfaces should be hit with unexpected inputs, Denial of Service (DoS) situations should be tested, unusual user activity should take place, and if a system crashes, the product should react by reverting back to a more secure state. The product should be tested in various environments with different applications, configurations, and hardware platforms. A product may respond fine when installed on a clean Windows 2000 installation on a stand- alone PC, but it may throw unexpected errors when installed on a laptop that is remotely connected to a network and that has an SMS client installed.

At this stage, issues found in unit and formal testing are relayed to the development team in problem reports. The problems are fixed and retesting occurs. This is a continual process until everyone is satisfied that the product is ready for production. If there is a specific customer, the company would run through a range of tests before formally accepting the product. Then the product is formally released to the market or customer. A totally different group of people should carry out the formal testing. This is an example of ***separation of duties***. A programmer should not develop, test, and release software. The more eyes upon the code and the more fingers punching keys, the greater the chance that bugs will be found before the product is released. The core components (sub-phases) of the testing phase are:

- ✓ **Black-box testing** observes the system external behavior.
- ✓ **White-box testing** is a detailed exam of a logical path, checking the possible conditions.
- ✓ **Compiled code** poses more risk than interpreted code because malicious code can be embedded in the compiled code and can be difficult to detect.
- ✓ **Regression testing** is the verification that what is being installed does not affect any portion of the application system already installed. It generally requires the support of automated process to repeat tests previously undertaken.
- ✓ **Code comparison** is normally used to identify the parts of the source code that have changed.
- ✓ **Integration testing** is aimed at finding bugs in the relationship and interfaces between pairs of components. It does not normally test all functions.
- ✓ **Unit testing** is the testing of a piece of code. It will only detect errors in the piece of code being tested.

	TASK	OWNER
Build/Test	Ingrain compliance in Software/Hardware	Project Manager, System Developers, and Test Engineer
	Review & update compliance risk analysis	Project Manager, System Developers, and Test Engineer
	Develop testing compliance checklist	Project Manager, & Test Engineer
	Conduct compliance testing	System Developers and Test Engineer
	Perform compliance gate reviews	Project Manager, Test Engineer, & Quality Assurance Team
	Obtain approvals from stakeholders	Project Manager

Table 6 – Compliance Tasks - Build/Test Phase

Implementation Phase & Compliance

The implementation stage focuses on how to use and operate the developed system or application. At this phase, the customer has purchased the developed product and installed it into their environment. The product would then be configured for the right level of protection. Functionality and performance tests can be performed, and the results can be analyzed and compared with the company's security requirements. The configurations should be documented. User guides and operation and maintenance manuals are developed so users know how to properly use the systems, and so the technical staff knows how to properly configure the product if needed. Monitoring compliance activities needs to be performed to ensure that the system or application performs in the manner promised by the service level agreement. Accreditation should occur between the implementation and the beginning of operational use of the system or application. This process should follow a certification process, which formally or informally calls for the testing of all the security features to determine if they accomplish the required compliance needs. Certification is the process of reviewing and evaluating security controls and functionality. It is usually a task assigned to an outside, independent reviewer. The accreditation is the formal acceptance of the system by management and an explicit acceptance of risk. The accreditation looks at the whole system, not just at an application or a newly upgraded feature. This is because security is not a compartmentalized attribute, but is a service that takes place at different layers of the system and can be manifested in many ways. The accreditation process forces the management and technical staff to work together to ensure quality and a level of protection provided by purchased and implemented technologies. The technical staff understands operational and mechanical issues, and the management staff understands mission, financial, and liability issues. Collectively, they can add great value to the certification accreditation processes. Once they are sure of the security provided by the new system and understand and accept the risk, management should issue a formal accreditation statement. Auditing needs to be enabled and monitored, and contingency recovery plans and procedures should be

developed and tested to make sure the system and product react as planned in the event of a system failure or emergency situation.

	TASK	OWNER
Implementation	Post deployment testing (certification)	Project Manager & System Owners
	Perform final compliance gate reviews with key stakeholders	Project Manager & Quality Assurance Team
	Obtain approvals from stakeholders including Quality Assurance team	Project Manager
	Compliance process and procedure updates where necessary	Project Manager &Quality Assurance Team

Table 7 – Compliance Tasks - Implementation Phase

Maintenance Phase & Compliance

In this phase of compliance, the potential for exposure and vulnerabilities are much higher than earlier phases. The need to ensure product (hardware and/or software) implemented remain in compliance has increased exponentially. Operational assurance (compliance) is carried out by continually conducting vulnerabilities tests, monitoring activities, and auditing events. It is through operational assurance activities that an administrator learns of new vulnerabilities or security compromises, so the proper actions can take place. If major changes happen to the system, product, or environment, a new risk analysis may need to be performed along with a new certification and accreditation process. These major changes could include adding new systems and/or new applications, relocating the facility, or changing data sensitivity or criticality.

When it is time for "out with the old and in with the new," certain steps may need to take place to make sure this transition happens in a secure manner. Depending on the sensitivity level of the data held on a system, various disposal activities may be necessary. Information may need to be archived, backed up to another system, discarded, or destroyed. If the data is sensitive and needs to be destroyed, it may need to be purged by overwriting, degaussing, or physically destroying the media. It depends on the data and the company's policy in destroying sensitive information.

	TASK	OWNER
Maintenance	Proper change control process	System owners
	Proper backup/recovery process	System owners
	Proper auditing/monitoring process	System owners
	Proper compliance policy	System owners

Table 8 – Compliance Tasks - Maintenance Phase

Assessment/Auditing

Periodic assessments of implemented critical systems (applications, database, operating systems, etc.) are to be conducted to determine the adequacy and effectiveness of established processes and procedures supporting them. Furthermore, assessment/auditing should help management ensure ongoing compliance and identify compliance risk conditions. Periodic assessment complements an organization's internal monitoring/quality assurance system; the board of directors should determine the scope of the assessment/audit, and the frequency with which it is conducted. The findings should be reported directly to the board of directors or a committee of the board. A written compliance report should include:

- ✓ Scope of audit (including departments, branches, and product types reviewed);
- ✓ Deficiencies or modifications identified;
- ✓ Number of transactions sampled by category of product type;
- ✓ Descriptions of or suggestions for, corrective actions and time frames for correction.

Board and senior management response to the audit report should be prompt. The compliance officer should receive a copy of all compliance reports, and act to address noted deficiencies and required changes to ensure full compliance with consumer protection laws and regulations. Management should also establish follow-up procedures to verify, at a later date, that the corrective actions were lasting and effective.

The compliance policy drives the methodologies that prescribe the processes and procedures that need to be assessed/audited. The assessment module has to ultimately address the main components (Information Security, Information System Change Control, Information Systems Development, and Information Systems Operations) of the policy. The assessment should be performed by resources that are not working on crafting and maintaining the major components (policies, methodologies, processes, and procedures) of the framework.

Logical Access/Information Security

Controls provide reasonable assurance that logical access to critical systems and applications is restricted to authorized personnel. Its main objectives are to:

- ✓ Determine whether or not only authorized security/account administrators (i.e., not end users) have the ability to create, modify, or delete access to critical systems.
- ✓ Determine whether or not user groups could grant, modify, or delete their own accesses.
- ✓ Determine whether or not accesses granted or changed by user account administration are authorized.
- ✓ Determine whether or not authorization for accesses to critical systems are documented/evidenced appropriately and maintained on file.

- ✓ Determine whether or not access levels are granted, modified, and terminated as appropriate to the user's job function.
- ✓ Determine whether or not employees/contractors who transfer job functions are identified and appropriate action taken to revalidate/suspend access to critical systems.
- ✓ Determine whether or not terminated employees/contractors are identified and their access removed.
- ✓ Determine whether or not employees/contractors have conflicting roles. e.g. the ability to submit and approve a credit.
- ✓ Determine whether or not the use of group IDs (generic) is adequately controlled.
- ✓ Determine whether or not accesses (User IDs and passwords) to critical systems are secure.
- ✓ Determine whether or not passwords for critical systems are changed from their default values.
- ✓ Determine whether or not access rights to critical systems are reviewed and confirmed periodically.
- ✓ Determine whether or not requests to delete or modify accesses to critical systems are processed completely and timely.
- ✓ Determine whether or not proper mechanisms/methods are used by the systems to authenticate application users.
- ✓ Determine whether or not resources performing this function are properly trained and supporting documentations (M&P and Job-Aids) are maintained and readily available.

Change Control/ Information Systems Change Control

Controls provide reasonable assurance that changes, including urgent and configuration changes, to critical systems and applications are authorized, tested, approved, properly implemented into production, and documented. The information systems change control main objectives are to:

- ✓ Determine whether or not policies and procedures that define required acquisition and maintenance processes have been developed and maintained.
- ✓ Determine whether or not proper segregation of duties exist between groups coding changes and groups moving changes into production.
- ✓ Determine whether or not system changes are tested, reviewed, and approved by the appropriate stakeholders prior to implementation.
- ✓ Determine whether or not proper setup and implementation of system software does not jeopardize the security of data and systems.
- ✓ Determine whether or not formal change control procedures are followed.
- ✓ Determine whether or not requests for job scheduling changes and maintenance are standardized, documented, and are following formal change management procedures.
- ✓ Determine whether or not resources performing this function are properly trained and supporting documentations (M&P and Job-Aids) are maintained and readily available.

Methodologies/Information Systems Development

Controls provide reasonable assurance that developed or acquired critical systems and applications follow the right methodologies. The information systems development main objectives are to:

- ✓ Determine whether or not approved methodologies for hardware and software development or acquisition are maintained, reviewed, and changed in accordance to business need, government regulations, and industry mandates.
- ✓ Determine whether or not newly acquired or developed systems (hardware, software, and databases) are designed in accordance with the methodologies in place.
- ✓ Determine whether or not only tested and validated developed or acquired systems, applications, and databases are implemented into production.
- ✓ Determine whether or not proper resources (systems SME, Compliance SME, Quality Assurance, etc.) are participating in the development or acquisition or software and hardware.
- ✓ Determine whether or not proper risk management processes are in place.
- ✓ Determine whether or not resources performing this function are properly trained and supporting documentations (M&P and Job-Aids) are maintained and readily available.

Information Systems Operations

Controls provide reasonable assurance that data, transactions, and programs are backed up, and backup media is periodically tested. They further provide assurance that physical access to computer network equipment and storage media is restricted to authorized personnel and stored in a secure and environmentally controlled facility. Its main objectives are to:

- ✓ Determine whether or not backups of critical systems are taken periodically.
- ✓ Determine whether or not offsite facilities are used for the storage of backup media
- ✓ Determine whether or not proper mechanisms are in place for the recovery of critical systems in an event of an emergency or system failures.
- ✓ Determine whether or not proper mechanisms are used to protect data (encryption, masking, etc.) in backup facilities.
- ✓ Determine whether or not physical access to computer network equipment and storage media is restricted to authorized personnel and stored in a secure and environmentally controlled facility.
- ✓ Determine whether or not recovery processes are tested periodically in lab or test environment.
- ✓ Determine whether or not proper mechanisms are used to protect critical data (SOX, PCI, PII, CPNI, HIPAA, etc.) in transit and in storage.
- ✓ Determine whether or not environments processing critical data are hardened (firewalls protected, restricted access, etc.)

- ✓ Determine whether or not critical environment are periodically scanned for exposure/vulnerabilities and proper mechanisms are in place to address vulnerabilities.
- ✓ Determine whether or not applicable security-related patches and other fixes provided by operating system vendors, application vendors, and other trusted third parties are tested and implemented in a time frame appropriate with the associated risk.
- ✓ Determine whether or not documentations on system configuration are maintained in proper location and reviewed periodically.
- ✓ Determine whether or not resources performing this function are properly trained and supporting documentations (M&P and Job-Aids) are maintained and readily available.

Summary

This research has proposed the implementation of an integrated compliance framework to be used primarily in the data processing environment - a robust and systemic framework that harmonizes controls across the information technology industry to significantly reduce the cost associated with complying with regulations, industry mandates, and security requirements effectively and efficiently. The proposed framework will facilitate the institutionalization of compliance in the core components of the business by implementing a governance model driven from the top down. The model starts with the creation and enforcement of a policy which in turn drives the compliance methodology. The compliance methodology prescribes the processes and procedures that are in-turn supported by the assessment module.

This framework, if implemented as prescribed, should allow companies to conduct business at reduced risks while taking full advantage of their information, processes, and resources.

Chapter 5: Suggestions for Additional Work

Risk Calculator Module

The risk calculator module will provide the ability to analyze business policies, processes, procedures, and systems in the "Integrated Compliance Framework for Data Processing Applications" model through review and comparison of country-specific privacy regulations and mandates. Management needs both detailed operational reports and critical risks to help them decipher the trending and relevance of multiple metrics, compliance indicators, operational performance indicator, and risk indicators – in a single, intuitive, one page, easy to read report. The proposed model will focus mainly:

- ✓ Business level focus
- ✓ Trending
- ✓ Prioritization
- ✓ Consistent aggregation
- ✓ Leading, lagging, and neutral indicators

Assessment Toolkit

The Assessment Toolkit is a semi-automated tool that can be used to facilitate the assessment process. The tool, question/answer driven, will be designed to capture answers to a series of questions that are driven from the key components of the policy (Information Security, Information System Change Control, Information Systems Development, and Information Systems Operations) and perform some high level analysis using built-in algorithms and the "Risk Calculator Module" to generate a detail report on the compliance portfolio of a company.

The tool will identify process improvement opportunities and prioritize them by level of criticality and degree of exposure. Also, it will contain a risk/issue mitigation component that will facilitate the capturing, tracking, monitoring of mitigation plans and timelines. Management sign-off on the report and mitigation plans will be captured in auditable format for auditing purposes. The tool does not require enormous resources (software and hardware) to be assembled. It can be built using existing Microsoft product (MS Access) and spare capacity on existing servers. The detail reports will paint a holistic view of the company's compliance profile or lack there of regarding to any regulations or industry mandates.

References/Bibliography

Electronic Media:
Bumiller, Elisabeth (2002-07-31). "*Corporate Conduct: Bush Signs Bill Aimed at Fraud in Corporations*". Available from http://query.nytimes.com/gst/fullpage.html?res=9C01E0D91E38F932A05754C0A9649C8B63. Internet; accessed 13 June 2009

Bemberger, J. (June 1997), "*Essence of the Capability Maturity Model"*. IEEE Computer, p. 112-114. Available from http://www2.umassd.edu/swpi/processframework/cmm/cmm.html. Internet; accessed 8 May 2009.

CanWest News Service (March 30 2007). "*TJX says hackers stole info from millions*". Available from http://www.canada.com/cityguides/kamloops/story.html?id=47a568fd-0231-4377-a40a-6898184f29b0&k=69398. Internet; accessed 2 November 2009.

CIOInsight (2006-06-26), "*Computer Security: ChoicePoint's Lessons Learned".* Available from http://www.cioinsight.com/c/a/Past-News/Computer-Security-ChoicePoints-Lessons-Learned/. Internet; accessed 2 November 2009.

CompTIA (2005-04-11). "*Data protection and security are the biggest challenge for information* technology…" available from http://www.itsecurity.com/security.htm?s=1731. Internet; accessed 13 June 2009

ISO Available from http://www.iso.org/iso/home.htm. Internet; accessed 8 August 2009.

ITIL. Available from http://www.itil-officialsite.com/home/home.asp. Internet; accessed 8 May 2009.

Mckinsey & Company study commissioned by NYC Mayor Michael Bloomberg and U.S. Sen. Charles Schumer, (D-N.Y.), cites this as one reason America's financial sector is losing market share to other financial centers worldwide. Available from http://www.senate.gov/~schumer/SchumerWebsite/pressroom/special_reports/2007/NY_REPORT%20_FINAL.pdf. Internet; accessed 8 May 2009.

TechFAQ. Available from http://www.tech-faq.com/itil.shtml. Internet; accessed 8 August 2009.

Webinar/eSymposium:
Law, Investigation and Ethics Objectives (July 2009) by Brightalk through membership with the Information Systems Audit and Control Association (ISACA) organization

Applications and System Development Objectives (April 2008) by Brightalk through membership with the Information Systems Audit and Control Association (ISACA) organization

Books:
J. Davidson Frame, *Managing Projects in Organizations: How to make the best use of time, techniques, and people.* Jossey-Bass Inc., 2003

James J. DeLuccia IV, *IT Compliance & Controls - Best Practices for Implementation.* Wiley, John & Sons, Incorporated, 2008

Sanjay Anand, *The Sarbanes-Oxley Guide for Finance & Information Technology Professionals*. Booksurge/CLA, 2004